

Claim Amendment Summary

Claims pending

- At time of the Action: Claims 1-3, 5-13, 15, 16, 19-33 and 35-42.
- After this Response: Claims 1-3, 5-13, 15, 16, 19-33 and 35-42.

Canceled or Withdrawn claims: none.

Amended claims: 22 and 35.

New claims: none

Please amend claims 22 and 35 as follows:

1. **(PREVIOUSLY PRESENTED)** A method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising:

generating a first key having a first version number;

providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;

generating a second key having a second version number; and when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number;

wherein said keys comprise key data and executable code for decrypting tickets.

2. **(ORIGINAL)** The method of claim 1 wherein a different key is provided to each site, and wherein each key is encrypted for decoding at one site.

3. **(ORIGINAL)** The method of claim 1 and further including generating

1 a configuration file to track keys for each site.

2
3 4. (CANCELED).

4
5 5. (PREVIOUSLY PRESENTED) A computer readable medium
6 having instructions stored thereon for causing a computer to perform a method of
7 updating keys that decrypt login tickets that log a user into multiple sites, the method
8 comprising:

9 generating a first key having a first version number,
10 providing tickets encoded consistent with the first key, the ticket having a
11 version number corresponding to the first version number;

12 generating a second key having a second version number, and
13 when the second key becomes current at a site, providing tickets encoded
14 consistent with the second key, the ticket having a version number corresponding to
15 the second version number,

16 wherein said keys comprise key data and executable code for decrypting
17 tickets.

18
19 6. (ORIGINAL) A method of generating keys that decrypt login tickets
20 that log a user into multiple sites, the method comprising:

21 generating a first key in the form of an executable having a first version
22 number;

23 generating a second key in the form of an executable having a second version
24 number; and

25 providing an indication to a login server identifying which key is current for

1 each site such that the tickets are properly encoded.

2
3 7. (ORIGINAL) The method of claim 6 and further comprising
4 distributing the key to multiple login servers in a secure manner.

5
6 8. (ORIGINAL) The method of claim 6 and further comprising updating
7 a configuration file to track keys for each site.

8
9 9. (ORIGINAL) A computer readable medium having instructions
10 stored thereon for causing a computer to perform a method of generating keys that
11 decrypt login tickets that log a user into multiple sites, the method comprising:

12 generating a first key in the form of an executable having a first version
13 number;

14 generating a second key in the form of an executable having a second version
15 number; and

16 providing an indication to a login server identifying which key is current for
17 each site such that the tickets are properly encoded.

18
19 10. (ORIGINAL) A system that generates keys that decrypt login tickets
20 that log a user into multiple sites, the system comprising:

21 a key generator that generates a first key in the form of an executable having a
22 first version number and generates a second key in the form of an executable having
23 a second version number; and

24 means for providing information to a login server identifying which key is
25 current for each site such that the tickets are properly encoded.

1
2 11. (PREVIOUSLY PRESENTED) A method of updating keys that
3 decrypt login tickets that log a user into multiple sites, the method comprising:
4 generating a new key with an incremented version number;
5 sending the new key to a partner site for use in decoding tickets with the
6 incremented version number;
7 updating key and version information for a login server; and
8 generating tickets decodable by the new key when an indication that a key
9 having a previous version number has expired;
10 wherein said keys comprise key data and executable code for decrypting
11 tickets.
12

13 12. (PREVIOUSLY PRESENTED) A computer readable medium
14 having instructions stored thereon for causing a computer to perform a method of
15 updating keys that decrypt login tickets that log a user into multiple sites, the method
16 comprising:
17 generating a new key with an incremented version number;
18 sending the new key to a partner site for use in decoding tickets with the
19 incremented version number;
20 updating key and version information for a login server; and
21 generating tickets decodable by the new key when an indication that a key
22 having a previous version number has expired;
23 wherein said keys comprise key data and executable code for decrypting
24 tickets.
25

1 13. (PREVIOUSLY PRESENTED) A method of updating a key used to
2 decrypt tickets used to log into a site, the method comprising:

3 receiving an updated key with a new version number;

4 setting a time for an old current key having an old version number to expire;

5 making the updated key the current key;

6 wherein at least one of said keys comprise executable code for making the
7 updated key the current key.

8
9 14. (CANCELED).

10
11 15. (ORIGINAL) The method of claim 13 and further comprising
12 redirecting users attempting to log into the site using the old current key.

13
14 16. (PREVIOUSLY PRESENTED) A computer readable medium
15 having instructions stored thereon for causing a computer to perform a method of
16 updating a key used to decrypt tickets used to log into a site, the method comprising:

17 receiving an updated key with a new version number;

18 setting a time for an old current key having an old version number to expire;

19 making the updated key the current key;

20 wherein wherein at least one of said keys comprise executable code for
21 making the updated key the current key.

22
23 17. (CANCELED).

24
25 18. (CANCELED).

1
2 19. **(ORIGINAL)** A method of managing keys used to decrypt tickets for
3 logging onto a site, the method comprising:

4 receiving a first key with a first version number;
5 encrypting the first key using a hardware address;
6 changing a current key variable to the first version number;
7 receiving a new key with an incremented version number;
8 encrypting the new key using a hardware address; and
9 identifying the new key as the current key.

10
11 20. **(PREVIOUSLY PRESENTED)** The method of claim 19 and further
12 comprising setting a time for the first key identifying when such key may no longer
13 be used.

14
15 21. **(ORIGINAL)** The method of claim 20 wherein a user currently
16 logged in may continue to use the first key until the time expires.

17
18 22. **(CURRENTLY AMENDED)** The method of claim 20 wherein a
19 new user may only use a ticket corresponding to the second key when the second key
20 is made the current key.

21
22 23. **(ORIGINAL)** The method of claim 20 wherein the time is set to a
23 reauthorization time determined by the site.

24
25 24. **(ORIGINAL)** The method of claim 19 wherein a new user using a

1 previous version ticket will be redirected to obtain a ticket corresponding to the new
2 key following the new key being identified as the current key.

3
4 25. (ORIGINAL) The method of claim 19 wherein the new key is
5 identified as the current key by changing the current key variable to the second
6 version number.

7
8 26. (ORIGINAL) A computer readable medium having instructions
9 stored thereon for causing a computer to perform a method of managing keys used to
10 decrypt tickets for logging onto a site, the method comprising:

11 receiving a first key with a first version number;
12 encrypting the first key using a hardware address;
13 changing a current key variable to the first version number;
14 receiving a new key with an incremented version number;
15 encrypting the new key using a hardware address; and
16 identifying the new key as the current key.

17
18 27. (PREVIOUSLY PRESENTED) A method of updating keys used to
19 decrypt tickets used to log into multiple sites on a network, the method comprising:

20 generating a new key with a new version number to take the place of an old
21 key with an old version number;
22 storing the new key on a site to be logged into by a user;
23 changing a current key indication to the new key;
24 allowing current logged in users to continue using the old key; and
25 redirecting new users to a login server to obtain a ticket consistent with the

1 new key;

2 wherein keys are generated in an executable form which includes key
3 information as well as code for decrypting tickets using the key information.

4
5 28. (ORIGINAL) The method of claim 27 wherein the old key may be
6 used by current logged in users for a predetermined amount of time.

7
8 29. (ORIGINAL) The method of claim 28 wherein the predetermined
9 amount of time is no more than a reauthorization time by which a current user is
10 normally required to provide login information.

11
12 30. (ORIGINAL) The method of claim 28 wherein the predetermined
13 amount of time may be set to zero to force all current and new users to login with a
14 ticket consistent with the new key version.

15
16 31. (ORIGINAL) The method of claim 27 wherein the ticket contains a
17 version number consistent with the version number of the key which can decrypt it.

18
19 32. (ORIGINAL) The method of claim 27 wherein keys are encrypted by
20 the site using a hardware address, and stored by the site.

21
22 33. (ORIGINAL) The method of claim 27 wherein a new key is
23 generated based on a request of the site.

24
25 34. (CANCELED).

1
2 35. (CURRENTLY AMENDED) The method of claim 27 wherein the
3 keys are generated by an authentication server, ~~and~~ and are distributed to multiple
4 login servers for providing login tickets.

5
6 36. (PREVIOUSLY PRESENTED) A computer readable medium
7 having instructions stored thereon for causing a computer to perform a method of
8 updating keys used to decrypt tickets used to log into multiple sites on a network, the
9 method comprising:

10 generating a new key with a new version number to take the place of an old
11 key with an old version number;

12 storing the new key on a site to be logged into by a user;

13 changing a current key indication to the new key;

14 allowing current logged in users to continue using the old key; and

15 redirecting new users to a login server to obtain a ticket consistent with the
16 new key,

17 wherein the keys comprise key data and executable code for decrypting
18 tickets.

19
20 37. (PREVIOUSLY PRESENTED) A method of logging on to multiple
21 sites, the method comprising:

22 sending a first login ticket to a desired site, wherein the login ticket is
23 encrypted to be decoded by a first key having a first version number;

24 receiving an indication that the first key has expired;

25 obtaining a second login ticket from an authentication server, wherein the

1 second login ticket is encrypted consistently with a new key having a second version
2 number; and

3 sending the second login ticket to the site to log into the site;
4 whercin the keys comprise key data and executable code for decrypting
5 tickets.

6
7 38. (ORIGINAL) The method of claim 37 wherein the tickets contain a
8 version number which is readable without decryption.

9
10 39. (ORIGINAL) The method of claim 38 wherein the version number is
11 a one digit Hex 5 integer.

12
13 40. (ORIGINAL) The method of claim 38 wherein the encrypted ticket
14 comprises an unencrypted version number, and encrypted information sufficient to
15 log a user into a desired site.

16
17 41. (PREVIOUSLY PRESENTED) A computer readable medium
18 having instructions stored thereon for causing a computer to perform a method of
19 logging on to multiple sites, the method comprising:

20 sending a first login ticket to a desired site, wherein the login ticket is
21 encrypted to be decoded by a first key having a first version number;

22 receiving an indication that the first key has expired;

23 obtaining a second login ticket from an authentication server, wherein the
24 second login ticket is encrypted consistently with a new key having a second version
25 number; and

1 sending the second login ticket to the site to log into the site;
2 wherein the keys comprise key data and executable code for decrypting
3 tickets.

4
5 42. (PREVIOUSLY PRESENTED) An encrypted ticket for use in
6 logging on to a website, the ticket comprising:

7 an unencrypted version number corresponding to a key version number stored
8 on the website; and

9 an encrypted string identifying the website and information, which when
10 decrypted using the key having the same version number authenticates the user for
11 logging the user into the website;

12 wherein the key comprises executable code for decrypting tickets.
13
14
15
16
17
18
19
20
21
22
23
24
25